AMENDMENTS TO THE CLAIMS

Claims 1-42 (Cancelled)

Claim 43 (Currently Amended) A recording apparatus for recording encrypted content onto a recording medium having a read-only unrewritable area and a rewritable area to which data can be recorded and from which data can be read, the recording apparatus being one component of a digital work protection system including a plurality of reproduction apparatuses that each attempt to decrypt the encrypted content recorded onto the recording medium, the recording apparatus comprising:

a device key storing unit operable to store a device key assigned to the recording apparatus;

a storage unit operable to store a piece of key revocation data that includes a plurality of encrypted media keys, each of the plurality of encrypted media keys respectively being generated by encrypting one media key with a corresponding device key of a plurality of device keys, the plurality of device keys being assigned to respective unrevoked apparatuses ~~each encrypted media key being generated (i) for a respective unrevoked apparatus of a plurality of unrevoked apparatuses and (ii) by encrypting a media key based on a device key assigned to the respective unrevoked apparatus~~;

a comparing unit operable to confirm whether or not the piece of key revocation data exists in the rewritable area of ~~on~~ the recording medium, the confirmation being made when content is to be recorded onto the recording medium;

a content encrypting unit operable to encrypt the content, based on a content key, to generate the encrypted content, the content being a piece of digital data;

a key encrypting unit operable, when the comparing unit confirms that the piece of key revocation data does not exist in the rewritable area of the recording medium, to (i) obtain an encrypted media key, from the plurality of encrypted media keys stored in the storage unit, that corresponds to the recording apparatus, when the recording apparatus is not revoked, (ii) ~~to~~ generate a media key by decrypting the obtained encrypted media key with the device key stored in the device key storing unit, and (iii) generate an encrypted content key by encrypting the content key based on [[a]] the generated media key ~~obtained, using the device key stored in the device key storing unit, from the piece of key revocation data stored in the storage unit, the encrypted content key being generated when the comparing unit confirms that the piece of key revocation data does not exist on the recording medium~~; and

a writing unit operable to record the encrypted content, the encrypted content key, and the piece of key revocation data that includes the plurality of encrypted media keys stored in the storage unit onto the rewritable area of the recording medium, the encrypted content, the encrypted content key, and the piece of key revocation data being recorded onto the rewritable area of the recording medium when the comparing unit confirms that the piece of key revocation data does not exist in the rewritable area of ~~on~~ the recording medium.

Claim 44 (Currently Amended) The recording apparatus of claim 43,

wherein, when the content is to be written onto the recording medium, the comparing unit confirms whether or not (i) a piece of key revocation data having a generation that is the same as a generation of the piece of key revocation data stored in the storage unit, or (ii) a piece of key revocation data having a generation that is different from the generation of the piece of key revocation data stored in the storage unit, exists on the recording medium,

wherein the key encrypting unit encrypts the content key based on the generated media key obtained from the piece of key revocation data stored in the storage unit, to generate the encrypted content key, when the comparing unit confirms that neither of (i) the piece of key revocation data having the generation that is the same as the generation of the piece of key revocation data stored in the storage unit and (ii) the piece of key revocation data having the generation that is different from the generation of the piece of key revocation data stored in the storage unit, exist on the recording medium, and

wherein the writing unit records the encrypted content, the encrypted content key and the piece of key revocation data stored in the storage unit to the rewritable area of the recording medium, when the comparing unit confirms that neither of (i) the piece of key revocation data having the generation that is the same as the generation of the piece of key revocation data stored in the storage unit and (ii) the piece of key revocation data having the generation that is different from the generation of the piece of key revocation data stored in the storage unit, exist on the recording medium.

Claim 45 (Previously Presented) The recording apparatus of claim 44, wherein the comparing unit confirms whether or not either of (i) the piece of key revocation data having the generation that is the same as the generation of the piece of key revocation data stored in the storage unit and (ii) the piece of key revocation data having the generation that is different from the generation of the piece of key revocation data stored in the storage unit, exist in the rewritable area of the recording medium.

Claim 46 (Currently Amended) The recording apparatus of claim 44, ~~further comprising:~~

wherein the [[a]] the comparing unit compares ~~unit operable to compare~~ the piece of key revocation data recorded on the recording medium with the piece of key revocation data stored in the storage unit to judge which of the piece of the key revocation data stored in the recording medium and the piece of key revocation data stored in the storage unit is newer, the comparing unit performing the comparison when the comparing unit confirms that either of (i) the piece of key revocation data having the generation that is the same as the generation of the piece of key revocation data stored in the storage unit and (ii) the piece of key revocation data having the generation that is different from the generation of the piece of key revocation data stored in the storage unit, exist on the recording medium~~; and~~,

wherein the recording apparatus further comprises an updating unit operable to update the piece of key revocation data stored in the storage unit, and

wherein, when the comparing unit judges that either of (i) the piece of key revocation data having the generation that is the same as the generation of the piece of key revocation data stored in the storage unit and (ii) the piece of key revocation data having the generation that is different from the generation of the piece of key revocation data stored in the storage unit, exist on the recording medium and when the comparing unit judges that the piece of key revocation data recorded on the recording medium is newer, the updating unit reads the piece of key revocation data from the recording medium and updates the piece of key revocation data stored in the storage unit with the piece of key revocation data read from the recording medium.

Claim 47 (Currently Amended) The recording apparatus of claim 46,

wherein, when the comparing unit confirms that either of (i) the piece of key revocation data having the generation that is the same as the generation of the piece of key revocation data

stored in the storage unit and (ii) the piece of key revocation data having the generation that is different from the generation of the piece of key revocation data stored in the storage unit, exist on the recording medium and when the comparing unit judges that the piece of key revocation data recorded on the recording medium is older, the key encrypting unit further encrypts the content key based on the generated media key obtained from the piece of key revocation data stored in the storage unit, to generate the encrypted content key, and

wherein the writing unit further records the encrypted content key to the rewritable area of the recording medium.

Claim 48 (Currently Amended) The recording apparatus of claim 47, further comprising:

a reading unit operable to read the encrypted content key from the rewritable area of the recording medium; and

a content key decrypting unit operable to (i) obtain an encrypted media key corresponding to the recording apparatus from the pluralty of encrypted media keys stored in the storage unit, when the recording apparatus is not revoked, (ii) generate a media key by decrypting the obtained encrypted media key with the device key stored in the device key storing unit, and (iii) decrypt the read encrypted content key based on the generated media key ~~obtained from the piece of key revocation data recorded to the recording medium,~~ to generate the content key,

wherein the key encrypting unit further encrypts the content key generated by the content key decrypting unit, based on the generated media key obtained from the piece of key revocation data stored in the storage unit, to generate the encrypted content key, and

wherein the writing unit further records the encrypted content key to the rewritable area of the recording medium.

Claim 49 (Previously Presented) The recording apparatus of claim 46,

wherein the piece of key revocation data stored in the storage unit includes a first piece of version information indicating the generation of the piece of key revocation data stored in the storage unit,

wherein the piece of key revocation data recorded on the recording medium includes a second piece of version information indicating the generation of the piece of key revocation data recorded on the recording medium, and

wherein the comparing unit judges which of, (i) the piece of key revocation data stored in the storage unit and (ii) the piece of key revocation data recorded on the recording medium, is newer by comparing the first piece of version information with the second piece of version information.

Claim 50 (Previously Presented) The recording apparatus of claim 46,

wherein the piece of key revocation data stored in the storage unit includes a first piece of time information indicating a time at which the piece of key revocation data stored in the storage unit was generated,

wherein the piece of key revocation data recorded on the recording medium includes a second piece of time information indicating a time at which the piece of key revocation data recorded on the recording medium was generated, and

wherein the comparing unit judges which of, (i) the piece of key revocation data stored in the storage unit and (ii) the piece of key revocation data recorded on the recording medium, is newer by comparing the first piece of time information with the second piece of time information.

Claim 51 (Previously Presented) The recording apparatus of claim 44,

wherein the piece of key revocation data stored in the storage unit further includes a first data identifier that identifies the piece of key revocation data stored in the storage unit, and

wherein the writing unit (i) records the first data identifier and the encrypted content to the rewritable area of the recording medium such that the first data identifier and the encrypted content are in correspondence, and (ii) records the piece of key revocation data including the first data identifier to the rewritable area of the recording medium.

Claim 52 (Currently Amended) The recording apparatus of claim 51,

wherein the recording medium includes another piece of key revocation data including another set of a plurality of encrypted media keys, the plurality of encrypted media keys of the another set respectively being generated by encrypting one media key with a corresponding device key of the plurality of device keys, the plurality of device keys being assigned to respective unrevoked apparatuses ~~each encrypted media key of the another set of encrypted media keys being generated (i) for a respective unrevoked apparatus of a plurality of unrevoked apparatuses and (ii) by encrypting a media key based on a device key assigned to the respective unrevoked apparatus~~,

wherein the another piece of key revocation data includes a second data identifier that identifies the another piece of key revocation data recorded on the recording medium, and

wherein the recording apparatus further includes an assigning unit operable to assign the first data identifier, which is different from the second data identifier, to the piece of key revocation data stored in the storage unit.

Claim 53 (Currently Amended) The recording apparatus of claim 51, ~~further comprising:~~

wherein the [[a]] comparing unit compares ~~operable to compare~~ the piece of key revocation data stored in the storage unit with the piece of key revocation data recorded on the recording medium to judge which of the piece of key revocation data stored in the storage unit and the piece of key revocation data recorded on the recording medium is newer~~, and~~, and

wherein the recording apparatus further comprises an assigning unit operable to assign the first data identifier to the piece of key revocation data stored in the storage unit when the piece of key revocation data stored in the storage unit is judged to be newer.

Claim 54 (Previously Presented) The recording apparatus of claim 53,

wherein the piece of key revocation data stored in the storage unit includes a first piece of time information indicating a time at which the piece of key revocation data stored in the storage unit was generated,

wherein the piece of key revocation data recorded on the recording medium includes a second piece of time information indicating a time at which the piece of key revocation data recorded on the recording medium was generated, and

wherein the comparing unit judges which of, (i) the piece of key revocation data stored in the storage unit and (ii) the piece of key revocation data recorded on the recording medium, is newer by comparing the first piece of time information with the second piece of time information.

Claim 55 (Currently Amended) A recording method used by a recording apparatus operable to record encrypted content onto a recording medium having a read-only unrewritable area and a rewritable area to which data can be recorded and from which data can be read, the recording apparatus being one component of a digital work protection system including a plurality of reproduction apparatuses that each attempt to decrypt the encrypted content recorded onto the recording medium, the recording method comprising:

storing, in a device key storing unit, a device key assigned to the recording apparatus;

encrypting content, based on a content key, to generate the encrypted content, the content being a piece of digital data;

storing, in a storage unit, a piece of key revocation data including a plurality of encrypted media keys, each of the plurality of encrypted media keys respectively being generated by encrypting one media key with a corresponding device key of a plurality of device keys, the plurality of device keys being assigned to respective unrevoked apparatuses ~~each encrypted media key being generated (i) for a respective unrevoked apparatus of a plurality of unrevoked apparatuses and (ii) by encrypting a media key based on a device key assigned to the respective unrevoked apparatus~~;

confirming, when the content is to be recorded onto the recording medium, whether or not the piece of key revocation data exists in the rewritable area of ~~on~~ the recording medium;

a key encrypting step of, when the confirming confirms that the piece of key revocation data does not exist in the rewritable area of the recording medium, (i) obtaining an encrypted media key, from the plurality of encrypted media keys stored in the storage unit, corresponding to the recording apparatus, when the recording apparatus is not revoked, (ii) generating a media key by decrypting the obtained encrypted media key with the device key stored in the device key storing unit, and (iii) generating an encrypted content key by encrypting the content key based on [[a]] the generated media key ~~obtained, using the device key stored in the device key storing unit, from the piece of key revocation data stored in the storage unit, the generating of the encrypted content key being performed when the confirming of whether or not the piece of key revocation data exists on the recording medium confirms that the piece of key revocation data does not exist on the recording medium~~; and

recording the encrypted content, the encrypted content key, and the piece of key revocation data that includes the plurality of encrypted media keys stored in the storage unit onto the rewritable area of the recording medium, the recording being performed when the confirming of whether or not the piece of key revocation data exists on the recording medium confirms that the piece of key revocation data does not exist in the rewritable area of ~~on~~ the recording medium.

Claim 56 (Currently Amended) A non-transitory computer-readable storage medium having a program stored thereon, the program for controlling a recording apparatus operable to record encrypted content onto a recording medium having a read-only unrewritable area and a rewritable area to which data can be recorded and from which data can be read, the recording apparatus being one component of a digital work protection system including a plurality of reproduction apparatuses that each attempt to decrypt the encrypted content recorded onto the

recording medium, and the program causing the recording apparatus to execute a method comprising:

storing, in a device key storing unit, a device key assigned to the recording apparatus;

encrypting content, based on a content key, to generate the encrypted content, the content being a piece of digital data;

storing, in a storage unit, a piece of key revocation data including a plurality of encrypted media keys, each of the plurality of encrypted media keys respectively being generated by encrypting one media key with a corresponding device key of a plurality of device keys, the plurality of device keys being assigned to respective unrevoked apparatuses ~~each encrypted media key being generated (i) for a respective unrevoked apparatus of a plurality of unrevoked apparatuses and (ii) by encrypting a media key based on a device key assigned to the respective unrevoked apparatus~~;

confirming, when the content is to be recorded onto the recording medium, whether or not the piece of key revocation data exists in the rewritable area of ~~on~~ the recording medium;

a key encrypting step of, when the confirming confirms that the piece of key revocation data does not exist in the rewritable area of the recording medium, (i) obtaining an encrypted media key, from the plurality of encrypted media keys stored in the storage unit, corresponding to the recording apparatus, when the recording apparatus is not revoked, (ii) generating a media key by decrypting the obtained encrypted media key with the device key stored in the device key storing unit, and (iii) generating an encrypted content key by encrypting the content key based on [[a]] the generated media key ~~obtained, using the device key stored in the device key storing unit, from the piece of key revocation data stored in the storage unit, the generating of the encrypted content key being performed when the confirming of whether or not the piece of key revocation~~

~~data exists on the recording medium confirms that the piece of key revocation data does not exist on the recording medium~~; and

recording the encrypted content, the encrypted content key, and the piece of key revocation data that includes the plurality of encrypted media keys stored in the storage unit onto the rewritable area of the recording medium, the recording being performed when the confirming of whether or not the piece of key revocation data exists on the recording medium confirms that the piece of key revocation data does not exist in the rewritable area of ~~on~~ the recording medium.

Claim 57 (Currently Amended) A non-transitory computer-readable storage medium comprising:

a read-only unrewritable area; and

a rewritable area to which data can be recorded and from which data can be read,

wherein a medium inherent number that is inherent to the computer-readable storage medium is prestored in the unrewritable area,

wherein a piece of key revocation data including a plurality of encrypted media keys, an encrypted content, and an encrypted content key are recorded in the rewritable area,

wherein each of the plurality of encrypted media keys respectively being generated by encrypting one media key with a corresponding device key of a plurality of device keys, the plurality of device keys being assigned to respective unrevoked apparatuses ~~each encrypted media key of the plurality of encrypted media keys is generated (i) for a respective unrevoked apparatus of a plurality of unrevoked apparatuses and (ii) by encrypting a media key based on a device key assigned to the respective unrevoked apparatus~~,

wherein the encrypted content is generated by encrypting content, based on a content key, to generate the encrypted content, the content being a piece of digital data, and

wherein the encrypted content key is generated by, when the piece of revocation data does not exist in the rewritable area, (i) obtaining an encrypted media key, from a plurality of encrypted media keys stored in a storage unit, corresponding to a recording apparatus, when the recording apparatus is not revoked, (ii) generating a media key by decrypting the obtained encrypted media key with a device key assigned to the recording apparatus and stored in a device key storing unit, and (iii) generating ~~encrypting~~ the encrypted content key based on [[a]] the generated media key ~~obtained using a device key assigned to a recording apparatus~~.

Claim 58 (Currently Amended) A digital work protection system comprising:

a recording apparatus for recording encrypted content onto a recording medium having a read-only unrewritable area and a rewritable area to which data can be recorded and from which data can be read; and

a plurality of reproduction apparatuses, each reproduction apparatus being operable to attempt to decrypt the encrypted content recorded onto the recording medium,

wherein a piece of key revocation data and an encrypted content are recorded in the rewritable area of the recording medium,

wherein the piece of key revocation data includes a plurality of encrypted media keys, each of the plurality of encrypted media keys respectively being generated by encrypting one media key with a corresponding device key of a plurality of device keys, the plurality of device keys being assigned to respective unrevoked apparatuses ~~each encrypted media key being generated (i) for a respective unrevoked apparatus of a plurality of unrevoked apparatuses and~~

~~(ii) by encrypting a media key based on a device key assigned to the respective unrevoked apparatus,~~

wherein the encrypted content is generated by encrypting content based on a content key, the content being a piece of digital data,

wherein the recording apparatus includes:

a device key storing unit operable to store a device key assigned to the recording apparatus;

a content encrypting unit operable to encrypt the content, based on the content key, to generate the encrypted content;

a storage unit operable to store the piece of key revocation data;

an comparing unit operable to confirm whether or not the piece of key revocation data exists in the rewritable area of ~~on~~ the recording medium;

a key encrypting unit operable, when the comparing unit confirms that the piece of key revocation data does not exist in the rewritable area of the recording medium, to (i) obtain an encrypted media key, from the plurality of encrypted media keys stored in the storage unit, corresponding to the recording apparatus, when the recording apparatus is not revoked, (ii) ~~to~~ generate a media key by decrypting the obtained encrypted media key with the device key stored in the device key storing unit, and (iii) generate an encrypted content key by encrypting the content key based on [[a]] the generated media key ~~obtained, using the device key stored in the device key storing unit, from the piece of key revocation data stored in the storage unit, the encrypted content key being generated when the comparing unit confirms that the piece of key revocation data does not exist on the recording medium~~; and

a writing unit operable to record the encrypted content, the encrypted content key, and the piece of key revocation data that includes the plurality of encrypted media keys stored in the storage unit onto the rewritable area of the recording medium, the encrypted content, the encrypted content key, and the piece of key revocation data being recorded onto the rewritable area of the recording medium when the comparing unit confirms that the piece of key revocation data does not exist in the rewritable area of ~~on~~ the recording medium, and

wherein each reproduction apparatuses includes:

a reading unit operable to read the piece of key revocation data recorded onto the rewritable area of the recording medium or read part of the piece of key revocation data recorded onto the rewritable area of the recording medium;

a decrypting unit operable to decrypt an encrypted media key from the piece or part of key revocation data read by the reading unit, the decrypting unit decrypting the encrypted media key using the device key assigned to the reproduction apparatus, to generate a decryption media key; and

a decrypting unit operable to read the encrypted content from the recording medium and decrypt the read encrypted content based on the generated decryption media key, to generate decrypted content.

Claim 59 (Previously Presented) The recording apparatus of claim 44, wherein, when the comparing unit judges that either of (i) the piece of key revocation data having the generation that is the same as the generation of the piece of key revocation data stored in the storage unit and (ii) the piece of key revocation data having the generation that is different from the generation of the piece of key revocation data stored in the storage unit, exist on the recording

medium and when the comparing unit judges that the piece of key revocation data recorded on the recording medium is not newer, the updating unit does not read the piece of key revocation data from the recording medium and does not update the piece of key revocation data stored in the storage unit with the piece of key revocation data read from the recording medium.

Claim 60 (Previously Presented) The recording apparatus of claim 43, wherein the piece of key revocation data recorded by the writing unit includes one encrypted media key corresponding to the recording apparatus and includes other encrypted media keys corresponding to the unrevoked apparatuses except the recording apparatus.